esper

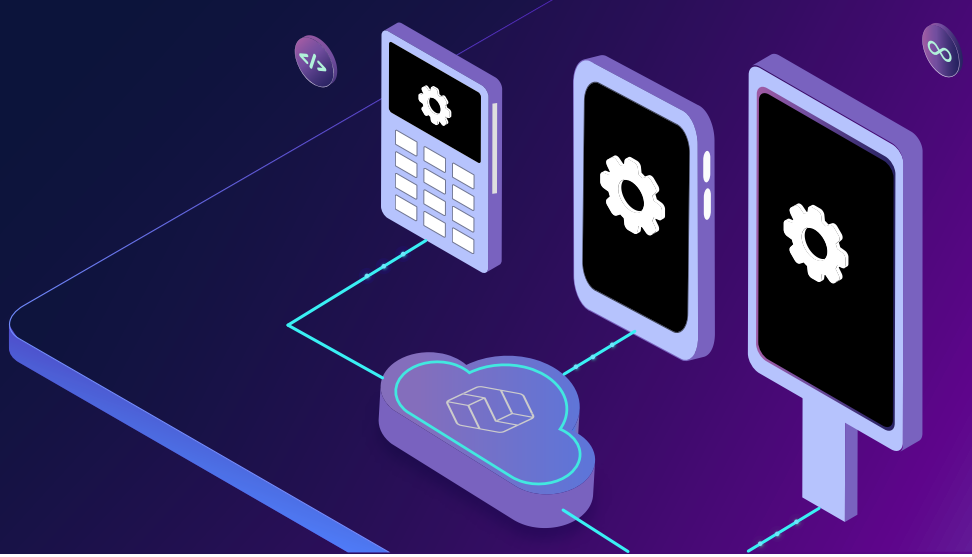
What is MDM?

Everything You Need to Know About Mobile Device Management

Digital devices are everywhere in modern businesses — everything from customer-facing devices like kiosks and digital signage to critical management tools like tablets, smartphones, and laptops. Tech-first companies need a way to manage and track these devices, but they also need to scale and grow quickly. That's where MDM comes in.

Table of Contents

What is MDM?



MDM stands for Mobile Device Management — a category of software tools that organizations of all sizes use to monitor and protect their devices. For some, it could mean managing employee devices on a company network. For others, it could mean managing business-critical devices like kiosks or point-of-sale. There's no one-size-fits-all MDM solution, and each device management scenario needs to be evaluated individually.

And that's an important distinction: MDM is not the same as "managing devices." One is a software tool (MDM), and the other is an action (device management) done using an MDM tool. It's no longer just about mobile phones — MDM software has become a blanket term for all different kinds of device management.

Overview and Key Features of Mobile Device Management Tools

In the modern sense, mobile device management is generally one part software and one part hardware. MDM software manages the hardware — you can't have one without the other in scenarios with managed devices. Mobile device management software utilizes security policies to protect crucial data and other content, as well as protect devices from malicious software (malware), ransomware, or other attacks. This is mobile device management as a service, which uses a cloud-based SaaS (software as a service) model instead of the more outdated on-premises model.

Modern MDM features include a number of core tools for remote management, asset tracking, and more. Some common examples include:

- **Remote configuration, control, and troubleshooting:** On-prem management options don't work for modern organizations, so remote tools are commonplace among MDM software providers. The level at which these tools are available will vary between vendors, but at the bare minimum, you should expect a way to remotely configure and monitor devices.
- **Device tracking:** Nearly all modern digital devices have a location-based feature, which is crucial for asset management and tracking. With a good MDM, you can pinpoint where any device in your fleet is at any given moment.

Application and content management:

As the needs we place on devices grow, managing on-device content is crucial. App distribution and content management tools are paramount — and we're not just talking about slapping an always-on app store on the device. Granular tools to protect devices from unauthorized installations and downloads are part of the package, too.

Operating system (OS) update and security patch management:

Similar to app and content management tools, a way to granularly control system updates and security patches is important. This allows you to schedule updates for off-peak hours, ensure your devices are always running the latest security patches, and more.

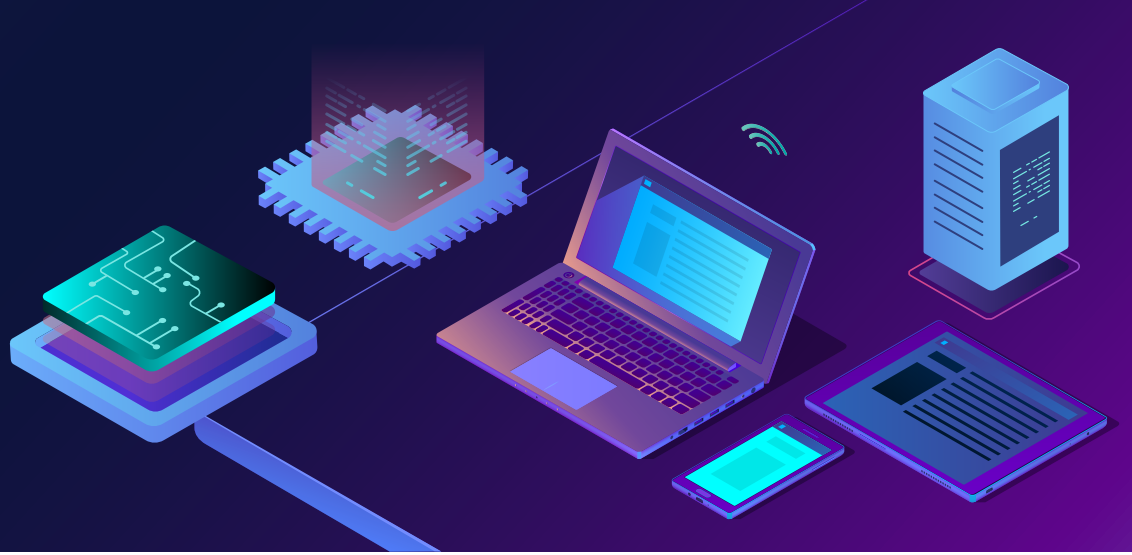
Health monitoring:

Asset tracking is just one part of the picture when it comes to monitoring devices — you also need insight into how those devices perform. Detailed telemetry data can give insight into device health, including performance, battery, and more. This allows you to spot potential issues before they become problems and optimize your devices based on usage stats.

While this is far from an exhaustive list, it's a great starting point when evaluating MDM providers. But, as with most things, it's far from the only consideration you need to make. MDM services commonly support various operating systems, including Android, iOS, iPadOS, Windows, macOS, and (in some cases) Linux. OS-specific solutions may integrate more tightly into the platform in which they're designed to work.

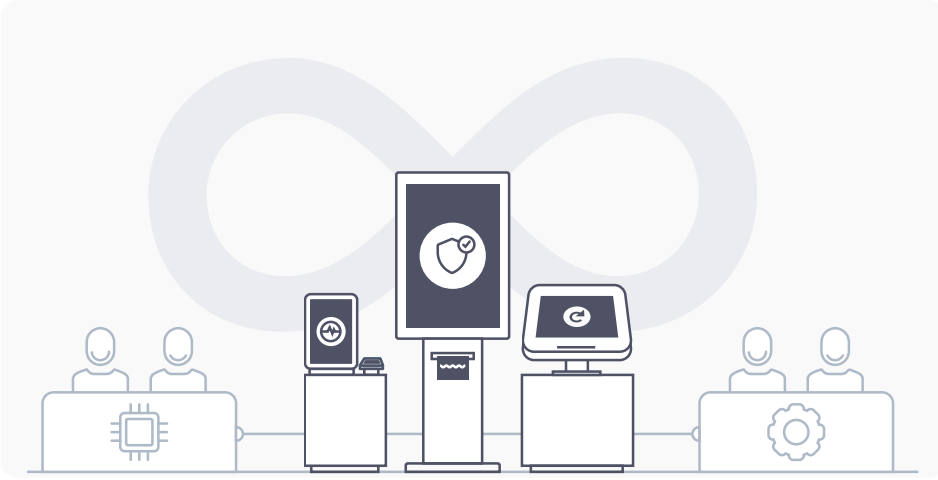
It's important to consider your specific device management needs and explore options that encompass the many facets of MDM as a whole.

Types of Device Management Tools: MDM, MAM, EMM, and UEM



The first MDM offerings were specifically for mobile devices (i.e., not desktop computers), which led to the creation of other types of management software, like MAM (Mobile Application Management), EMM (Enterprise Mobility Management), and UEM (Unified Endpoint Management). As organizations adopt more types of devices, the need for more advanced management tools was born. Here's a quick breakdown:

- **MAM:** Mobile Application Management. This is used to secure, update, and monitor applications on devices.
- **EMM:** Enterprise Mobility Management. This is a more robust MDM designed for enterprise users. Think of it as MDM + MAM.
- **UEM:** This was originally designed to manage computers and company networks. Today, most UEMs also support mobile devices.
- **MDM:** This was originally designed for employee smartphones on company networks but has since branched out to cover nearly all types of digital devices, like tablets, computers, and more. The term "MDM" is often used as a blanket term to cover all other types of management software, like MAM, EMM, and UEM.

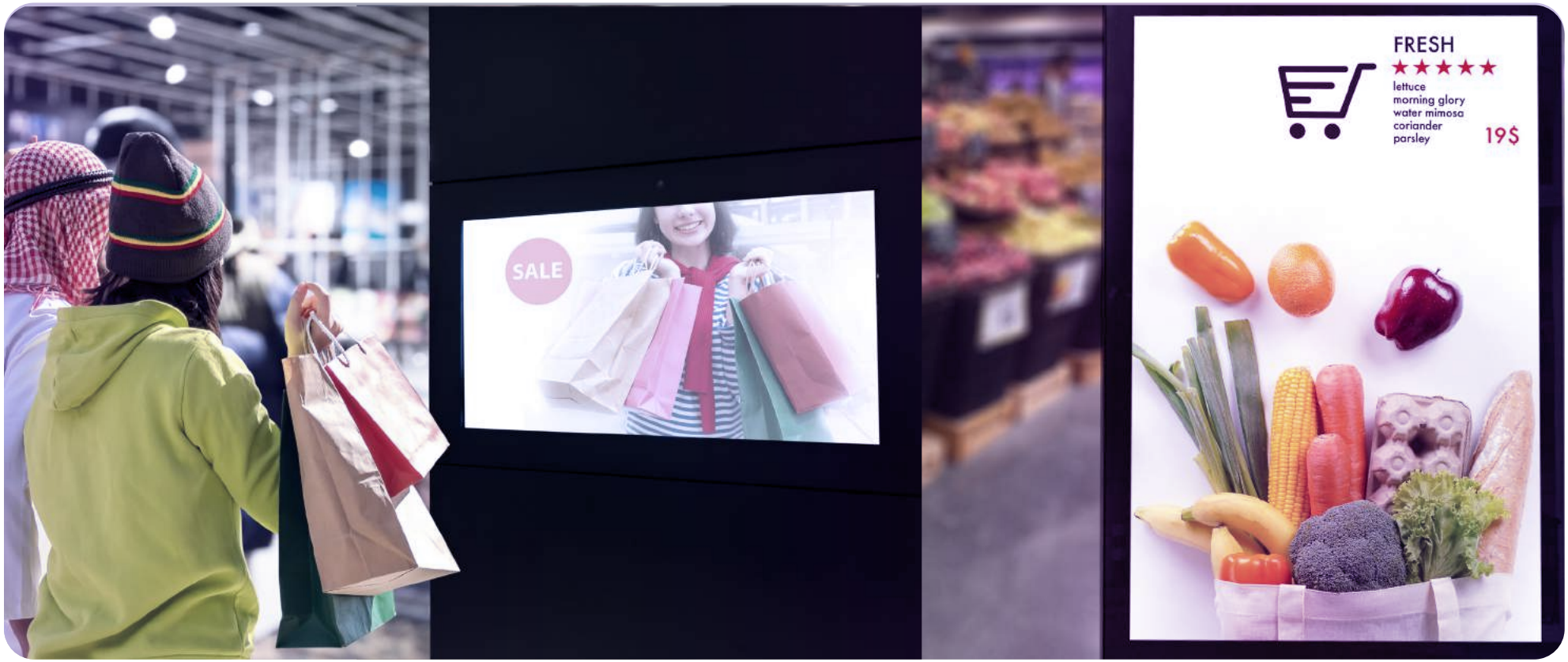


Here's a chart that breaks down MDM, MAM, EMM, and UEM. When looking at it, keep in mind that we're focusing on the traditional aspect of MDM here. Modern MDM encompasses nearly all of these components, but it's still important to note the historical distinctions!

FEATURES	MDM	MAM	EMM	UEM
Smartphone management	✓	✓	✓	✓
Device tracking & geofencing	✓	✗	✓	✓
Application management	✗	✓	✓	✓
Remote troubleshooting	✓*	✗	✓*	✓*
Data security	✓	✓	✓	✓
Remote configurations & updates	✓	✗	✓	✓
Computer management	✗	✗	✗	✓
Advanced Telemetry & diagnostics	✗	✗	✗	✗
App delivery automation	✗	✓*	✓*	✗
Remote configuration & deployment	✓*	✗	✓*	✓*
Device grouping	✗	✗	✗	✗

***** – *only basic functionality is supported***

Now that we've established terms, from this point forward, we'll talk about MDM in the modern sense — as an all-encompassing umbrella that covers the functionality from all of the subcategories. With that, let's talk about common features found in modern MDM tools.



Common Components of MDM Software

Not all MDM software is created equal, but there are some foundational components you should find across every device management provider worth its salt. Technology stacks will vary across different providers and software tools, and the depth of each feature could also change from service to service, but this is the "if they don't have it, run away" list. Ya feel me?

- **Device provisioning:**
  It's impossible to provide MDM tools without proper provisioning. In the simplest terms, device provisioning is defined as "setting up a device to work in a specific manner." The depth in which you go to achieve said status can be as shallow as tweaking a few settings or as intricate as replacing the entire operating system. Either way, every MDM service out there will offer a way to provision and onboard (or enroll) the device to its platform.

- **Policy management:**
  In MDM terms, policy management is the ability to define, enforce, and manage rules and configurations across mobile devices. This means you can set policies and enforce them according to organizational standards and security hygiene.

- **Mobile security:**
  This goes hand in hand with policy management but deserves its own point because robust mobile security is about more than just policy enforcement. Strong device security starts with your MDM and the security practices it adheres to, so ensure you thoroughly audit key considerations when evaluating providers.

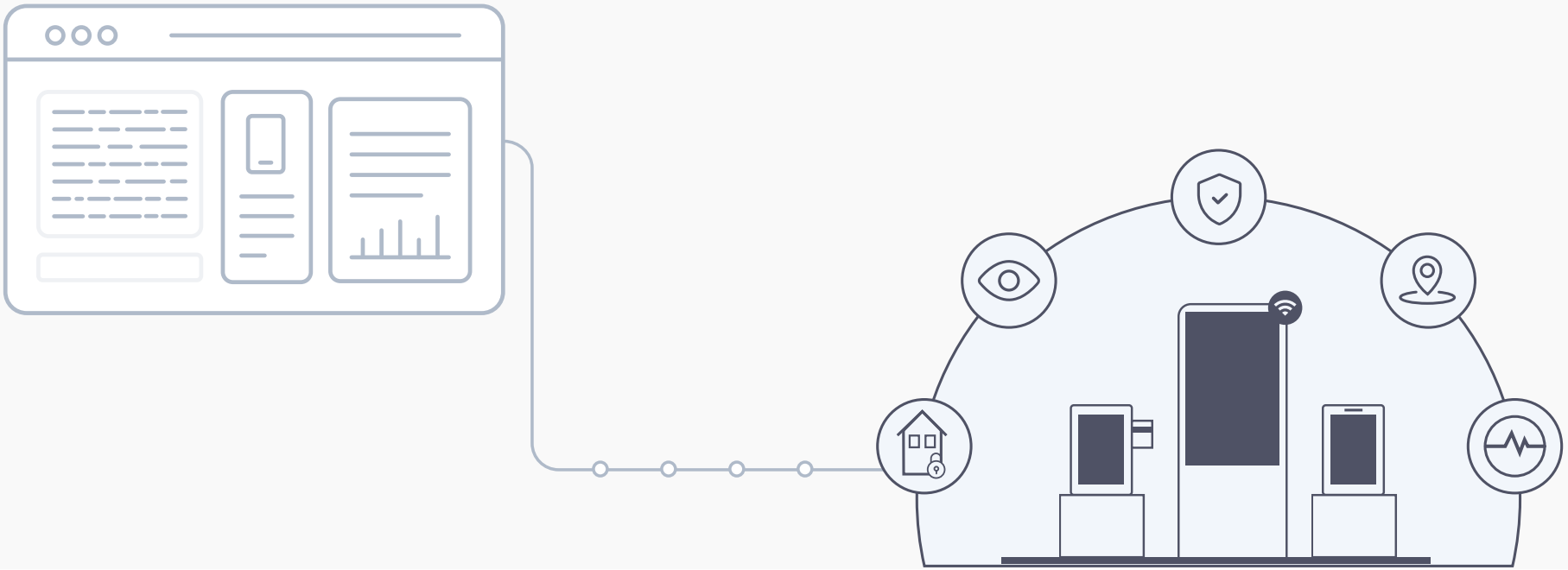
- **RBAC:**
  Role Based Access Control (RBAC) is a crucial feature that allows your MDM provider to scale with your business, as it allows for simpler account management by granting users customizable access according to their role. Specific roles will vary according to each service, but even pre-set roles are table stakes.

Reporting and analytics:

Despite the name, device management is about more than just managing devices. It's also about getting proper information about those devices — usage statistics, health info, geolocation, and all that good stuff are part of the package, too. This type of information is vital to a healthy, scalable device fleet.

That's yet another starting point – the types of devices you're managing and what they're used for will play a big part in determining what features you need from your MDM. For example, the needs of BYOD (Bring Your Own Device) and COPE (Corporate Owned, Personally Enabled) organizations will vary dramatically from the needs of COBO (Company Owned, Business Only) and COSU (Company Owned, Single Use) devices. And that's where we get into the nitty gritty of MDM intricacies.

Learn more about MDM security



Types of Devices MDM is Designed For

When managing mobile devices, there's no shortage of options. But it all starts with what type of devices you need to manage according to your business model. And in many cases, your needs may overlap. Here's a quick breakdown of each before we dive into the specifics:

- **BYOD:**
  Bring Your Own Device. This is for organizations that allow employees to use their own devices but still need a way to protect corporate data. BYOD is most commonly used on smartphones, tablets, and laptops.

- **COBO:**
  Corporate Owned, Business Only. This is for company-owned hardware that is exclusively used for business purposes. You'll find this on things like office computers..

- **COPE:**
  Corporate Owned, Personally Enabled. The company officially owns these devices but allows employees to also use them for personal use. You'll commonly see COPE uses on employer-issued smartphones and laptops.

- **COSU:**
  Corporate Owned, Single Use. This class is also called "dedicated devices" — these are similar to COBO devices, but they have a single, distinct function and never deviate from that functionality. Think POS systems or smart barcode scanners here.

The last two types of device management are also called "fully managed," meaning the organization owns, operates, and manages these devices.

BYOD and COPE: The Backbone of Device Management Software

As mentioned earlier, MDM software started as a way for organizations to manage smartphones — namely in a BYOD scenario. This was when portable devices started to take off, and people were using them more and more for work (remember Blackberry?), so companies needed a way to protect their sensitive data. Traditional MDM was born out of the need for a way to control that data on BYOD devices.

As digital devices started to proliferate across businesses, COPE was also born. The company owns these devices, but they're not locked down or heavily restricted, so employees can use them for personal and business use. Company-issued smartphones and laptops are ideal candidates for COPE environments, but tablets also fit the bill.

COBO and COSU: Modern Devices Require Modern Tools

There will always be a need for MDM providers that service BYOD and COPE organizations, but this type of device management software simply isn't ideal for business-critical devices. The always-on, business-first hardware that many modern organizations rely on requires a different approach to management than BYOD or COPE. Thus, MDM providers that service COBO and COSU devices were born.

These devices transcend traditional MDM services because they're owned by the business, used by the business, and focused on the business. They're never personally enabled and typically only run a single or small number of applications. Interestingly, there can be dramatic overlap between the types of devices found across all four device management categories.

For example, smartphones are increasingly common in COBO and COSU environments, as they're incredibly versatile. Laptops and tablets also fall into both of these categories as well. Where you start to see more deviation is hyper-specific hardware that is purpose-built and business-critical. We're talking about things like POS systems, digital kiosks, digital signage, and more. These are all perfect examples of COBO and COSU devices.

This is the type of device management that Esper specializes in. The always-on, hyper-connected devices that businesses rely on.

As mentioned above, many businesses rely on multiple types of device management services, as they have BYOD or COPE needs and COBO and COSU. They have employee devices and business devices. Never the two shall meet. Because why would they? They have dramatically different purposes.

This is exactly why different types of device management exist. And the benefits across all of them are pretty easy to pinpoint.

Benefits of Mobile Device Management Software

It's hard to overstate the importance of Implementing a cohesive device strategy with a strong device management partner. There are a multitude of benefits here, especially in an age where digital devices are everywhere (and spreading). Here are some top reasons to adopt an aligned device management strategy.

- **Centralized management tools:** When everything is in one place, it makes life easier. With the right device management service, you can monitor every aspect of your device fleet from a single pane of glass — everything from usage metrics to remote diagnostics. Boom, baby.

- **Enhanced security:** Full control means just that — control. Not just over the devices themselves but the update strategy, patch management, and more. All these things collectively make for a more secure system, which is more important than ever.

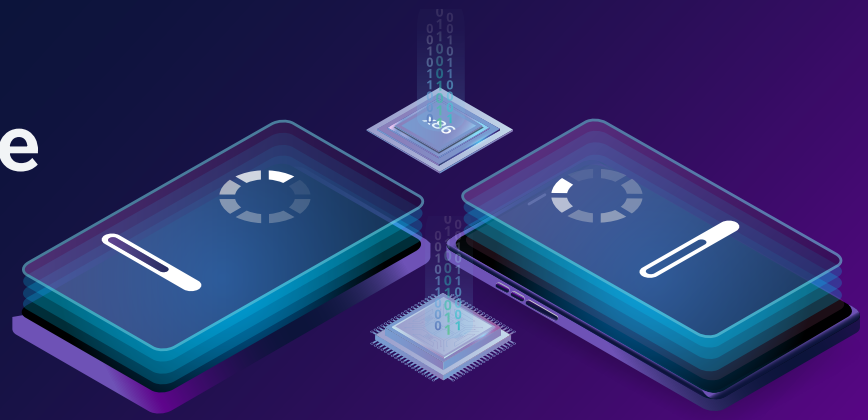
- **Remote monitoring, configuration, and troubleshooting:** Seeing what your devices are doing from afar is one thing, but reacting to those things is a different story altogether. A strong MDM solution will allow you to address both aspects — monitoring first and troubleshooting second. All without leaving your desk.

- **App and content management:** In the modern device scene, apps and content make the world go 'round. Because of that, you need control of those apps and the content. The ability to change or modify content on the fly and control app distribution — even down to specific app versions — is more important than ever.

- **Compliance and reporting:** A proper device strategy is the opposite of set-and-forget. You also need a way to gather reports about device activity, gain real-time alerts when things exceed set parameters, and do deep audits of device health. And when things are askew, quickly getting them back into compliance with drift management is a must.

Having a device strategy that doesn't involve robust, reliable management simply doesn't work — you need both to utilize your hardware most effectively. Of course, there are two sides to every coin.

Challenges of Mobile Device Management Software



For all its benefits, several challenges are associated with implementing an MDM solution. Often, you can mitigate these with the proper approach, but you need to consider and adjust for it on the front side. With that, here are a few things to chew on before you dive in.

- **Device diversity and scalability:** The more device types you have, the more flexible your MDM solution needs to be. Managing a fleet of 100 tablets is pretty straightforward, but that can quickly change if you try to implement a new device type (or, in some cases, even a different brand of tablet!). Having a solution that fits your needs now and in five years can be challenging.
- **Migration from other MDMs:** This goes hand-in-hand with the above point — if your current device management solution is lacking, you'll need to switch to another. This is often laborious and time-consuming.
- **Implementation and adoption:** Onboarding a new device management tool can be tough on its own, and that's before you even get to the user adoption aspect. As with anything new and seemingly different, there will always be resistance from users. You'll need to decide on a way to encourage adoption ahead of time in order to maximize the ease of transition. Good MDM providers usually offer onboarding and enablement to help with the transition.
- **Integration:** Again, MDM goes beyond just your device and the users. Third-party software and peripherals also need to play nicely with your chosen device management solution, which sometimes doesn't even hit the radar until it's too late. That's why it's a good idea to inventory all of your software and peripherals ahead of time. You can thank us later.
- **Security compliance:** That's a double-edged sword, huh? On one hand, you get enhanced security from a strong MDM. On the other, this enhanced security can be problematic by hindering device capabilities or limiting access to resources. Sure, security is as tight as it can possibly be, but at what cost?

Good device management is a balancing act. You want tight security, but users also need to be able to do what the device was intended for. You want to scale easily, but don't want to pay for more than you need. You need to quickly implement a reliable MDM solution, but don't have to get it right the first time. We get it. It's hard — and we've seen it a lot.

Where Most MDM Options Start to Break Down

Remember that time we said not all MDMs are created equal? Well, let's dive into that. If you're looking for a device management tool for COBO or COSU but end up going with something designed for BYOD, well, you're not going to have a very good experience. And that works both ways. There are a lot of MDM options out there that simply fall apart when it comes to fully managed devices, so if that's your bag, this section is for you.

- **Advanced remote troubleshooting and debugging:** Sure, you have insight into what's happening with your devices. But what happens when something goes wrong? Maybe a simple reboot fixes it, but maybe it's more. Most MDM software doesn't offer the tools you need for truly advanced remote troubleshooting and debugging. We're talking about full remote control, sure, but also remote command line, APIs, and all that jazz.

- **Dynamic device grouping:** Ever tried to manage a device fleet in the thousands without the ability to group similar devices together? It's rough. That's why dynamic grouping by device, location, OS version, or anything else that makes sense is something you should have. You'll wonder how you ever lived without it.

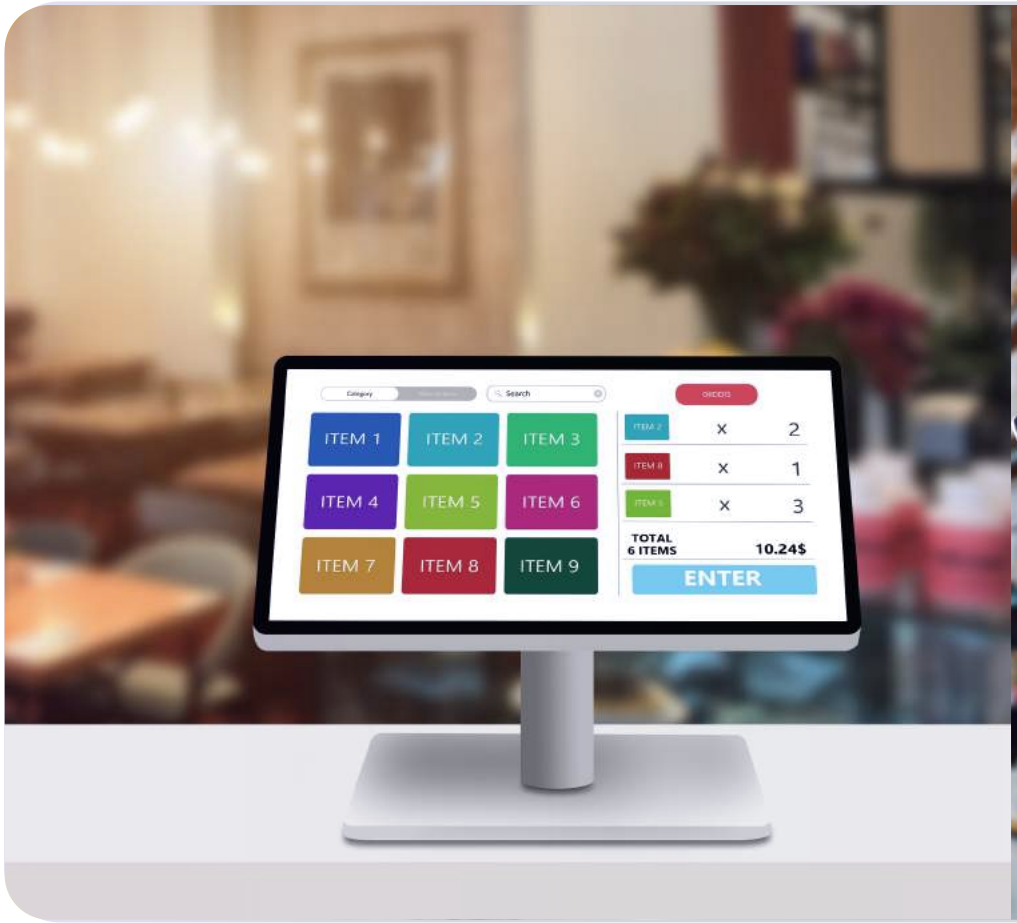
- **Granular app version control:** What if we told you that running the same version of your app across every device in your fleet isn't a great idea? Okay, maybe if you have hundreds of the exact same device, it's fine. But if you're like most, your fleet is full of different devices, which means different hardware and even operating system versions. That's why app version control is absolutely clutch for the modern device fleet.

- **Custom configurations and templatized policy implementation:** Provisioning new hardware can be a real pain. Re-provisioning hardware for a different use can be even worse. That's why a dynamic, customizable, reusable, templatized approach to configuration and policy is implementation is the way forward — and an area where many MDM providers simply fall short.

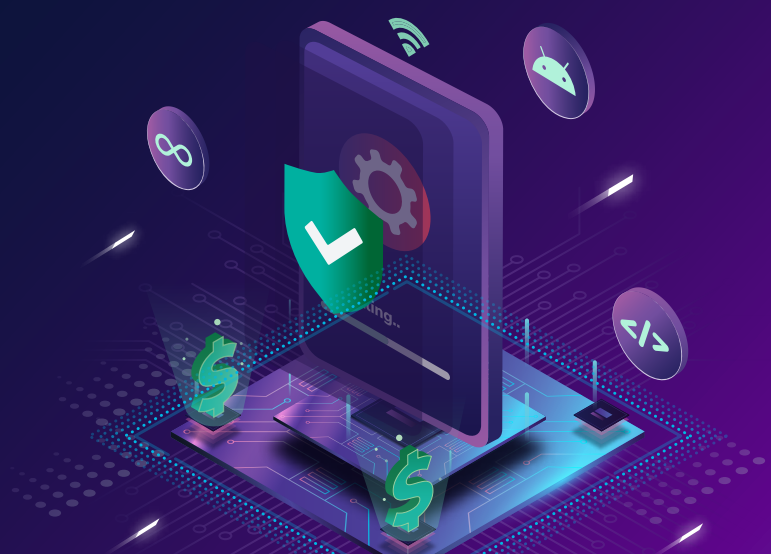
Fully remote and touchless deployments:

When it comes to deploying devices, many MDM providers lean toward on-site deployments. Remote deployments are the future of MDM implementation, and if you really want your mind blown, a truly touchless deployment is where it's at.

Trying to use an MDM provider that was built for yesterday's use-cases in today's world will leave you wanting in many cases. This is especially true for company-managed devices — the revenue-generators that drive innovation forward. That's why it's good to take a step or two back and truly evaluate what you need. You'll likely find that it's time to go beyond MDM in the traditional sense.



Going Beyond Traditional MDM Software



Modern devices and use cases require modern device infrastructure. That last word is the one to pay attention to here: infrastructure. Today's businesses need more than the basic MDM software, so a full-stack, integrated solution that marries hardware and software with robust management tools is the way to connect the missing pieces. This is what it's like to transcend MDM.

Sure, transcendence is about the tools involved, but that's just the start. A truly integrated experience is about a smarter approach to device management. **Full automation** of repetitive tasks or intelligent responses to trigger-based alerts is a great example here. Imagine never having to think about your devices and what happens if one goes offline, for example. With the right tools, a device could automatically reboot when no connection is detected — that's the first thing an IT tech is going to do anyway. Automation paves the way for a more efficient way forward.

That's where a **full-stack solution** starts to take shape. You might be asking yourself, "What does full-stack mean in the context of device management?" which is a valid question. A full-stack device management solution is end-to-end. It starts with hardware at the edge and ends in an intuitive, user-friendly console on the other side —- and it covers everything in between. Imagine a future where your hardware, software, and device management all work together in harmony.

When we say "everything in between," we mean it. **APIs and SDKs** that simplify implementing new apps or new app versions make your developers' lives easier. **Secure remote debugging and diagnostics** simplify troubleshooting for IT teams without fear of security vulnerabilities. Both of those things combined make for unified dev and IT teams, leading to increased productivity and faster throughput.

For device managers, **robust device grouping** is the way to keep like-devices together. Want to update all your POS devices at once? Or how about every device at a specific location? Oh, you need to send a very specific APK to a small group of older devices across the country? You got it. You're out there playing chess while everyone else is playing checkers.

That's what the future of device management looks like.

The Importance of Picking the Right MDM Provider

At this point, one thing should be clear: your MDM provider matters. Go with the wrong one, and it's something you potentially have to live with for years. Pick the right one, and suddenly everything about your device strategy becomes easier — scaling is smoother, compatibility is a non-issue, and your **TCO is immediately clear.**

TCO considerations for MDM

Ah, but the devices themselves are a double-edged sword, right? That's why **hardware compatibility** is the first step to choosing the right MDM. Some device management providers want to lock you in to their hardware that only works with their MDM, offering the combo under the illusion of a "platform." And that's all well and good until you want to deviate from their (usually limited) hardware selection.

That's a non-starter for many organizations because **scalability** is critical for the modern device fleet. As our reliance on digital devices becomes more prolific, the need to seamlessly and fluidly manage those devices is equally important. You need to be able to scale quickly and without worry. That doesn't just apply to your devices, either — **integration with third-party apps and peripherals** is part of the puzzle, too. Will your old barcode scanners work with the new POS? Crossing your fingers only goes so far.

But that's why a **partnership with your device management provider** is the cornerstone of this whole thing. The right MDM will enable you to scale quickly, offer valuable insights into hardware compatibility (read: let you choose the hardware that works best for your situation), and work with you to make sure all your third-party tools are compatible with the hardware selection. When it all clicks, it's pure harmony.

That's also where **TCO comes in**. The total cost of ownership extends past just your hardware, and the best MDM providers out there will make that clear. How does that super affordable tablet scale? Is it compatible with your thermal printers? Oh, and what happens when it breaks down (because these things happen) — does it support all the best remote tools? A device that doesn't do what you want it to do isn't very cost-effective and ultimately ends up costing you a lot more in the long run.

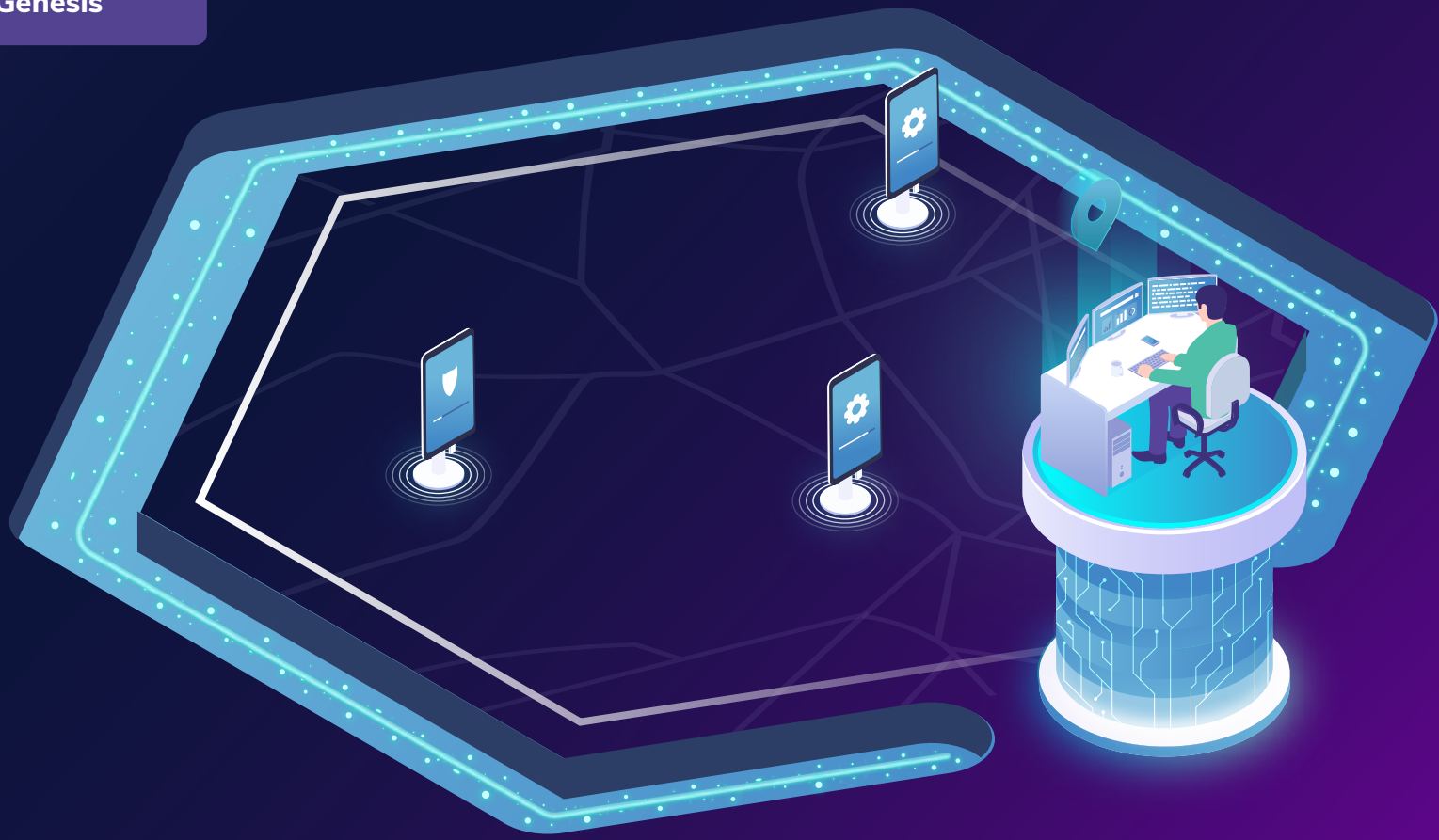
So yeah, picking the right device management partner is crucial because it ultimately impacts everything else around your device strategy.

Esper MDM Features and Tools

Esper understands MDM and where it falls short for modern device uses. That's why we took a smarter approach to device management with our entry-level MDM platform, Esper Genesis. With Genesis, you get all of the modern device management features you need, groundbreaking configuration tools that you won't find anywhere else, and the foundation to quickly scale when you're ready.

Genesis is the fluff-free MDM your company-managed devices deserve.

Learn more about Esper Genesis



esper

About Esper

Esper is on a mission to power exceptional device experiences by revolutionizing the way companies manage their device fleets. Through advanced capabilities, such as remote control & debugging, Pipelines for software deployment, Esper device SDK and APIs, Blueprints for dynamic configuration, and Seamless Provisioning, Esper is leading the market beyond standard MDM practices into the modern era of DevOps for devices and beyond. Recognized as one of Deloitte Technology Fast 500, Esper's innovative solutions support some of the world's most innovative brands in retail, hospitality, logistics, healthcare, education, and more.

Learn More